Mashing Up, Wiring Up, Gearing Up:
Solving Multi-Protocol Problems in Identity

Eve Maler
eve.maler@sun.com
A few notes about me and this talk

- Some relevant affiliations/perspectives:

- The thoughts I'm presenting today are my own, on...
  - Today's complicated identity landscape
  - Opportunities and pain points in achieving success in federated identity
  - Experiences with Project Concordia as a forum for getting there faster
Not to belabor the point at this workshop, but...

- Identity must be made more portable!
- More precisely, identity-related *information* needs to cross domain boundaries and identity-related *tasks* need to be shared across them (= federated identity)
  - **What**: attributes, claims, authentication contexts, security contexts, entitlements
  - **How**: easily, robustly, efficiently, and securely, with fidelity, trust, privacy, and scale
  - **Why**: user experience, personalization, access control, bottom-line savings, and new business models
It's not just about SSO and account linking

- Though they are major use-case drivers
SOA needs federated identity too

- Identity in distributed computing offers the ability to:
  - Get around browser payload limitations
  - Let multiple services cooperate securely on a person's behalf
  - Allow actions to happen “silently” when the person is not online, in a way that is...  
    - Mediated by policy
    - Protective of privacy
    - Auditable
One reason this is important

Consider the realities that medical professionals face today:

It's 2 a.m. You're here.

Your medical records are locked away here.

The ER doctor has 2 minutes to decide which one of these two injections won't cause a lethal allergic reaction.
Ways in which the real world intrudes on these objectives

- Heterogeneity is everywhere
  - Application platforms
  - Protocols (standardized and otherwise)
  - Legacy systems
  - Devices at the network's edge

- Technical issues are swamped by business and regulatory issues

- Users often act in ways “experts” wish they wouldn't
“[Specification], defined by [Spec Definition Body], has been optimized to support [Use Case] identity. Work is under way to create software libraries at [Open Source Project]. There will be an interop demonstration of [Specification] and [Specification] working together, as profiled at [Metasystem Initiative] at [Conference/Meeting]. Meanwhile, bickering continues on [Discussion Group].”

– adapted from Paul Madsen's ConnectID
We've seen some consolidation...

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td>Liberty bases new federation standard on emerging SAML standard.</td>
</tr>
<tr>
<td>2003</td>
<td>Liberty tracks SAML evolution; Internet2 Shibboleth bases its solutions on SAML also; Microsoft and partners publish WS-Federation 1.0.</td>
</tr>
<tr>
<td>2004</td>
<td>Liberty contributes ID-FF to OASIS for SAML2 convergence; Shibboleth also takes part.</td>
</tr>
<tr>
<td>2005</td>
<td>Liberty endorses SAML2 as its identity federation solution and provides interop and conformance testing; Shibboleth is working on new SAML2-based APIs.</td>
</tr>
<tr>
<td>2006</td>
<td>Microsoft and partners publish WS-Federation 1.1; OASIS TC formed May 2007.</td>
</tr>
</tbody>
</table>
We've seen some consolidation...

- **2003**: WS-Security, SAML TP 1.0
- **2004**: ID-WSF 1.0
- **2005**: ID-WSF 1.1
- **2006**: ID-WSF 2.0

- Liberty ID-WSF uses WS-Security before the ink is dry.
- ID-WSF revision takes into account new versions of underlying standards.
- Incorporates WS-Addressing Core/Bind 1.0 once standardized.
We've seen some consolidation...

2006

A number of technologies are explored for lightweight Internet identity

2007

OpenID 2.0 incorporates i-names and Yadis and is influenced by the others

OpenID

LID

inames

passel

Yadis
¿Quién es más meta?

- A hub service to handle translations between formats for security and identity tokens so that systems can communicate reliably?

![Diagram showing system interactions with token format exchanger and WS-Trust]

- System A: Token format A
- System B: Token format B
- System C: Token format C
- System D: Token format D
- Token format exchanger
- WS-Trust
¿Quién es más meta?

- Or a hub format for security and identity tokens that disparate systems can agree to use consistently?
- How about both?
So, some of the deployment challenges are...

- Complexity and feature duplication
- Differing models and abstractions between solutions
  - What information will persist, and what tasks can be performed, safely across them?
- Compliance and certification assurances
- Composability vs. interoperability
- Adoption trends for competing solutions
  - “Which horse to back”
Project Concordia offers one way to evolve past the strife

- Public forum
  - For deployers, who feel the pain
  - And vendors, who provide it...

- Deployers are use-case contributors
  - Similar to Liberty's gathering of market requirements

- Facilitate high-leverage solutions
  - Profiles and best practices
  - Educational materials
  - Testing out interop
Who is at the table?

- Use-case contributors so far
  - AOL, Boeing, Chevron, General Motors, Government of British Columbia, InCommon Federation, New Zealand State Services Commission, U.S. General Services Administration

- Sampling of representation from key vendors, OSS projects, protocol development efforts, and related communities
  - CardSpace, Microsoft, OSIS, SAML, Shibboleth, Liberty, OpenID, OAuth, WS-*...
Some common themes we're hearing from deployers

- Too many choices for federation!
- CardSpace futures with SAML and ID-WSF
  - As well as OpenID with ID-WSF...
- Handling impedance mismatches between WS-Federation and SAML2
- Scalable federation and interfederation
  - Need better metadata distribution and IdP discovery solutions
- Interoperability in conveying levels of assurance
One of the use cases from NZ

Shared Authentication Services

- Govt Logon Service
- Identity Verification Service
- Future Services

Persistent Pseudonyms

Identity via Browser SSO (SAML 2.0)

Identity Enabled WS (ID-WSF)

Govt Agency
One of the use cases from Boeing

- Web SSO Server
- IAM Proprietary
- LDAP Directory
- Federation Services

Employees

SAML, WS-Fed, OpenID?

Single federation interface for vendors and in-house developers?
Who needs to get smarter to handle heterogeneity?

- Different answers represent different use cases
- Previous technology choices made?
- Amount of control or influence over business partner and user behavior?
- Performance considerations?
- Number of federations each party has to deal with?
APIs vs. protocols – looking for “the truth”
Next steps for Concordia

- Add detail to highest-priority use case areas:
  - SAML2 + WS-Federation
  - (SAML/ID-WSF) + CardSpace
  - Federation rolled out at scale (Ping proposal)

- Propose improvements in:
  - Proxying/translation/switching
  - Metadata distribution and lifecycle
  - IdP discovery

- Work towards interop demonstrations during RSA conference in April 2008

- Continue to collect new use cases
An invitation to get involved

Why?
- Many other venues focus on prospective development, by vendors, of specs, APIs, mashups... – a very important role!
- Concordia is responding to deployers' needs and concerns about heterogeneous environments today
- If you have needs and concerns, we're here to help

How?
- www.projectconcordia.org
- Mailing list, wiki, workshops, telecons, interops
- Upcoming telecon (Nov) and workshop (Dec)
Thanks!
Questions?

Eve Maler
eve.maler@sun.com
www.xmlgrrl.com/blog
openid.sun.com/xmlgrrl :-)